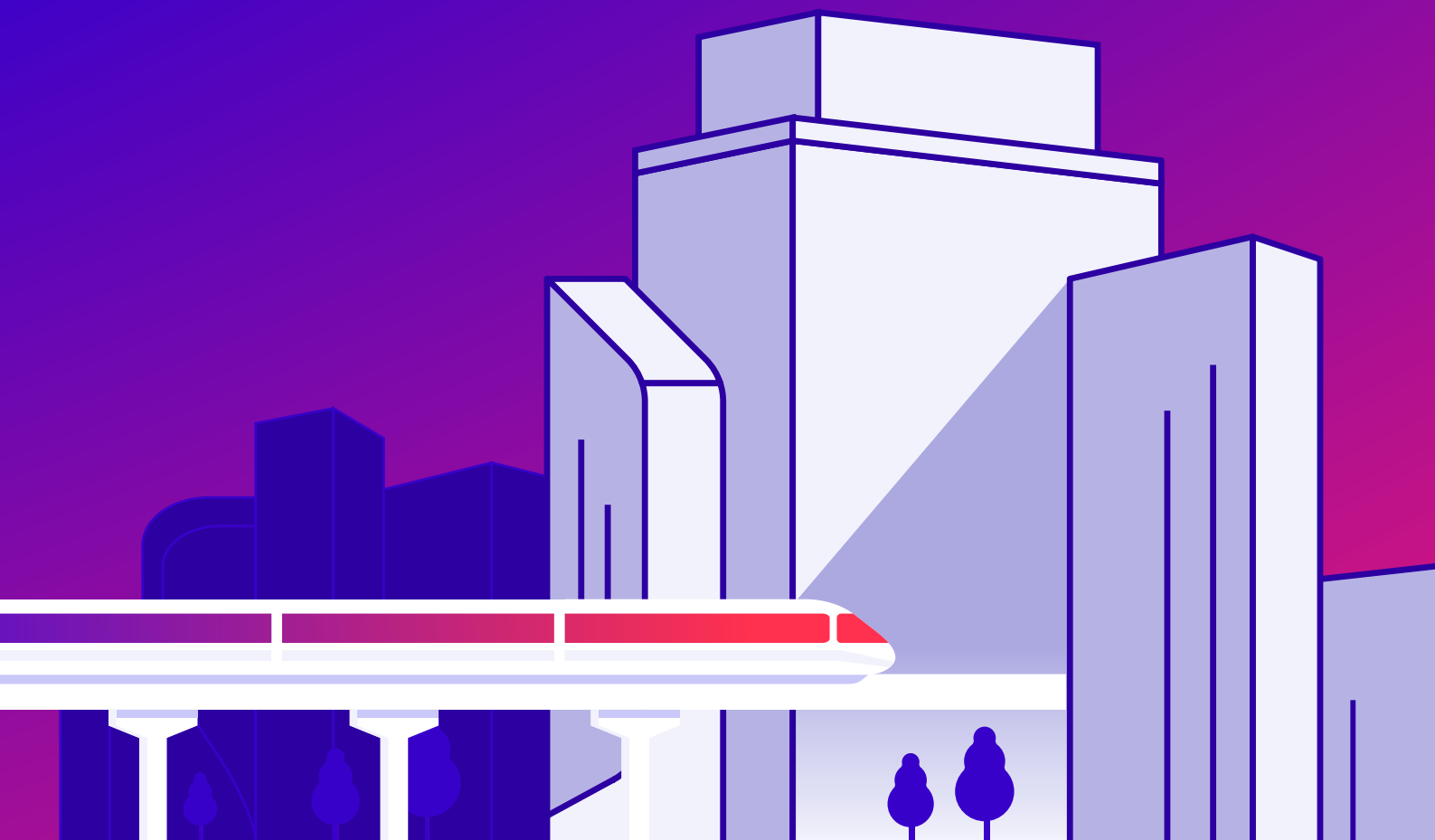




# Hong Kong Protection of Critical Infrastructure Bill

How Cymulate Exposure Management Accelerates Compliance



# Abstract

The *Hong Kong Protection of Critical Infrastructures (Computer Systems) Bill* introduces strict cybersecurity obligations across eight critical infrastructure sectors. This white paper examines how exposure management, powered by the Cymulate platform, accelerates compliance by ingesting and correlating asset and exposure data, continuously performing threat validation, identifying and prioritizing exploitable risks and aligning security strategies with regulatory requirements. By integrating asset discovery, security technologies, automated threat validation, contextual dashboards and reporting, Cymulate enables organizations, “CI operators” to streamline their compliance while strengthening their threat resilience.

## Table of Contents

<b>01</b>	<b>Introduction</b>	<b>3</b>
<b>02</b>	<b>Scope</b>	<b>3</b>
<b>03</b>	<b>Requirements and Non-Compliance</b>	<b>5</b>
<b>04</b>	<b>Exposure Management Accelerates Compliance</b>	<b>8</b>
<b>05</b>	<b>Implement Security Management Plan (Obligation 23)</b>	<b>9</b>
<b>06</b>	<b>Conduct Security Risk Assessments (Obligation 24)</b>	<b>10</b>
<b>07</b>	<b>Arrange Security Audits (Obligation 25)</b>	<b>10</b>
<b>08</b>	<b>Participate in Security Drills (Obligation 26)</b>	<b>10</b>
<b>09</b>	<b>Summary</b>	<b>10</b>

# 01

## Introduction

Cyber threats in Hong Kong are rapidly escalating, hitting a 5-year high with a 108 percent increase in data breach incidents in 2024 compared to 2023<sup>1</sup>. This surge in attacks heightens business risks and threatens the continuity of Hong Kong’s essential services. In response, the government passed the city’s first dedicated cybersecurity law, the *Protection of Critical Infrastructures (Computer Systems) Bill*, on March 19, 2025. Effective January 1, 2026, stronger protection of critical infrastructure and computer systems will be mandated to minimize service disruption and ensure continuity. This new law signals a new regulatory environment that elevates accountability, reinforces the importance of proactive defense and requires organizations to integrate security strategy with compliance.

The Hong Kong CI bill aligns with global cybersecurity standards, such as the US NIST Cybersecurity Framework (CSF) and the EU NIS2 Directive. It enforces proactive cybersecurity measures, such as risk assessments, incident reporting and security audits, and emphasizes continuous security validation of computer systems.

### Definition of Critical Infrastructure

Any infrastructure that is essential to the continuous provision in Hong Kong of an essential service in a designated sector, or any other infrastructure the damage, loss or functionality or data leakage of which may hinder or otherwise substantially affect the maintenance of critical societal or economic activities in Hong Kong.

# 02

## Scope

CI operators delivering services in the following eight designated critical infrastructure (CI) sectors must comply with the outlined obligations.



Energy




Information technology



Banking and financial services




Air transport



Land transport



Maritime transport



Healthcare services



Telecommunications and broadcasting services

<sup>1</sup> Source: HKCERT Unveils "Hong Kong Cyber Security Outlook 2025" Phishing Hits Five-year High Vulnerabilities in Supply Chain and AI Content Hijacking Emerge as Key Risks Over Half of Enterprises Fear Cyber Attacks on IoT Digital Signages

# 03

## Requirements and Non-compliance

Designated critical infrastructure (CI) operators must comply with the bill obligations, which are divided into three categories: organization, threat and incident preventive and incident reporting and response. CI operators who fail to comply with these obligations face significant monetary penalties, reaching up to HK\$5 million. In addition, organizations may be subject to additional daily fines for ongoing security breaches, compounding financial exposure until security deficiencies are fully addressed. Beyond financial penalties, there is a potential risk for heightened regulatory scrutiny and reputation damage.

These punitive measures highlight the seriousness with which Hong Kong regulators expect CI operators to manage cyber risk across critical sectors, such as energy, banking, telecommunications, transportation and healthcare. Compliance is not merely a technical checkbox but a strategic imperative for continued operational resilience.

### Organization Requirements

- Maintain office in Hong Kong
- Notify operator changes
- Establish and maintain computer-system security management unit

### Prevention of Threats and Incidents Requirements

- Notify of material changes to certain computer systems
- Submit and implement computer-system security management plan
- Conduct computer-system security risk assessments
- Arrange and carry out computer-system security audits

### Incident Reporting and Response Requirements

- Participating in computer-system security drills
- Submit and implement emergency response plan
- Notify of computer-system security incidents



“Cymulate allows organization to test and evaluate their security posture and controls. It makes it easier to identify (and fix) any issues BEFORE an audit or pen-test, instead of after, and most importantly, before a cybercriminal discovers and exploits your vulnerability.”

CISO, Health Organization



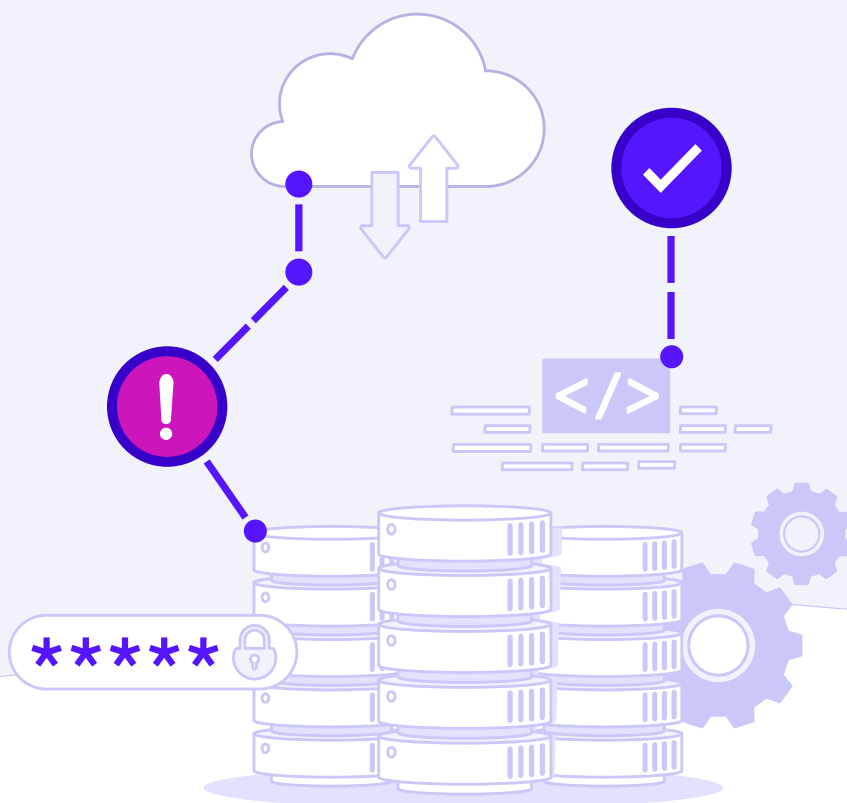
# 04

## Exposure Management Accelerates Compliance

Exposure management that combines asset discovery with automated security validation enables CI operators to continuously prove their exploitable threats. It allows them to systematically identify, assess, prioritize and mitigate their risks to critical infrastructure. With comprehensive exposure management incorporating threat validation, organizations accelerate compliance, gain real-time visibility and reporting, reduce the burden of periodic and manual audits and strengthen threat resilience. This ultimately minimizing disruption to essential services.

The Cymulate Exposure Management platform enables organizations to achieve strategic exposure management by providing a continuous, real-time view of their security posture, exploitable risks and resilience against emerging threats. Unlike traditional exposure management platforms that list known vulnerabilities and may prioritize with some level of threat intelligence, Cymulate continuously evaluates how real-world threats would behave in each unique environment, pinpointing not only existing weaknesses, but also where exploitable threats lack effective prevention or detection. Cymulate aggregates data and calculates true business risk to prioritize security and threat gaps to ensure CI operators mitigate their most critical security exposure risks before they can be exploited.

The Cymulate platform integrates with security technologies across endpoint, network, application, data and cloud, and asset discovery tools to comprehensively view assets and exposures. With Cymulate automated adversarial exposure validation (AEV), powered with breach and attack simulation (BAS), CI operators are equipped to easily schedule and run attack tests with the latest threat intelligence in their environments to identify their security prevention and detection gaps. These gaps are correlated with asset criticality, business impact and threat intelligence data to prioritize their mitigation efforts on their most critical risks, reducing the number of priority gaps to mitigate. Cymulate delivers actionable guidance and automated remediation for these exposure risks and accelerates detection engineering by generating new custom rules for easy implementation.



# 05

## Implement Security Management Plan (Obligation 23)

Obligation 23, categorized as a threat and incident preventive measure, requires CI operators to develop and implement computer-system security management plans that define the processes for protecting the security of critical infrastructure systems. Specifically, the processes should outline how CI operators will:

- Manage risk and vulnerabilities across the following areas: identify, assess, monitor and mitigate
- Protect information system and data
- Manage risks across all phases of the lifecycle

### CI operators are required to identify risks and vulnerabilities.

#### Cymulate capabilities:

**Vulnerability and exposure discovery integrations:** Integrating with asset discovery and exposure tools is essential to fully assess risk. Cymulate seamlessly connects with leading vulnerability scanners and exposure discovery solutions to provide a comprehensive view of organizational risk.

**Adversarial exposure validation:** The Cymulate platform integrates with existing security technologies to run automated attack simulations that test an organization's ability to prevent and detect threats. It identifies exploitable security gaps and maps them to the MITRE ATT&CK framework and other industry standards, enabling teams to clearly understand risks in the context across the attacker lifecycle.

**Attack path discovery:** Cymulate maps potential attack paths an adversary could exploit to access sensitive data, escalate privileges and move laterally across the environment. This capability enhances organizational visibility into security gaps and risks to critical infrastructure, enabling more effective defense and mitigation.

**Custom attacks:** CI operators are equipped to utilize intuitive workbenches to easily design and launch customized attacks, whether single-step or multi-staged. This capability enhances visibility into the effectiveness of existing mitigations and highlights risks most relevant to their specific environment(s).

**Phishing assessment:** Cymulate enables organizations to quickly automate phishing campaigns, providing clear insights into user susceptibility and phishing risks based on assessment results.

### CI operators are required to assess risks and vulnerabilities.

#### Cymulate capabilities:

**Exposure prioritization:** Cymulate enriches organization vulnerability and asset data with with business context, asset criticality, threat intelligence and prevention and detection findings to calculate true risk scores. This shifts organizations from theoretical risk to actionable insight by proving which exposures are truly exploitable in their environment. With a shared and prioritized view of risks, security operations, red teams, and vulnerability management teams can work more efficiently and focus remediation on their most critical exposures.

**MITRE ATT&CK coverage:** Cymulate maps each attack scenario to the corresponding MITRE ATT&CK techniques and sub-techniques and generates automated heat maps that visually display security coverage across the adversary lifecycle. CI operators are equipped to prioritize their risks and security gaps for each tactic to strengthen their overall defense in depth.

## CI operators are required to mitigate risks and vulnerabilities.

### Cymulate capabilities:

**Actionable mitigation guidance:** For validated and proven exploitable risks and security gaps, Cymulate provides prescriptive mitigation guidance, such as policy tuning recommendations and AI-powered insights. This empowers organizations to rapidly implement mitigations, optimizing security controls and improving threat resilience.

**Automated mitigation:** With security technology integrations, Cymulate allows organizations to easily push updates to their security controls for immediate threat prevention.

**Detection engineering:** Cymulate enables organizations to easily build, test and optimize threat detection with attack simulations and custom rules that automate detection engineering.

## CI operators are required to monitor risks and vulnerabilities.

### Cymulate capabilities:

**Continuous assessments:** Cymulate enables organizations to schedule automated assessments for continuous monitoring. By providing ongoing visibility into the effectiveness of security controls and emerging exploitable risks, CI operators can maintain strong threat resilience and ensure cybersecurity compliance.

**Security drift monitoring:** Cymulate enables organizations to monitor and track changes in their security posture by comparing new assessment results against previous baselines. This allows organizations to quickly identify emerging gaps, regressions or improvements over time.

## CI operators are required to protect information and data systems.

### Cymulate capabilities:

**Data protection validation:** The Cymulate platform has an extensive library of attack scenarios for CI operators to run and validate their data protection cybersecurity capabilities. Security teams receive actionable insights to quickly remediate data exposures to improve their overall data protection.

## CI operators are required to manage risks across the entire system lifecycle.

### Cymulate capabilities:

**System lifecycle risk management:** Organizations can evaluate their cybersecurity risks across the full system lifecycle – from development to maintenance. Attack tests can be executed during development and testing phases to identify risks and provide mitigation guidance, while continuous validation ensures security is maintained during the maintenance phase.

# 06

## Conduct Security Risk Assessments (Obligation 24)

Obligation 24, categorized as a threat and incident threat and incident preventive measure, requires CI operators to conduct penetration tests and vulnerability assessments every 12 months to proactively identify their vulnerabilities, impact and exploitable risk. CI operators are required to submit an assessment report.

### CI operators are required to conduct risk and vulnerability assessments.

#### Cymulate capabilities:

**Exposure validation automated assessments:** The Cymulate Exposure Management platform is the end-to-end solution for CI operators to conduct security risk and vulnerability assessments. Organizations conduct automated and continuous assessments to identify and prioritize exposures with a threat-based validation approach. With the Cymulate capabilities outlined in the obligations in section 05, which equips CI operators to develop and implement their risk and vulnerability management processes, this is the execution of the risk and vulnerability assessments with actionable mitigations and drift monitoring.

**Continuous proven threat resilience:** By continuously identifying and mitigating risk exposures and vulnerabilities, CI operators are equipped to optimize security controls and continually prove their threat resilience with outcome-driven metrics. This results in risk reduction to cyberattacks and their potential to cause severe damage and disrupt essential services.

### CI operators are required to prepare and submit a security risk assessment report.

#### Cymulate capabilities:

**Assessment dashboards and reports:** Cymulate automatically generates dashboards and reports with metrics and charts that can be used in the report. The platform allows for customization to meet organization-specific needs.

# 07

## Arrange Security Audits (Obligation 25)

Obligation 25, categorized as a threat and incident threat and incident preventive measure, requires CI operators to arrange computer-system security audits, executed by independent auditors, every 24 months. These audits verify that system protections have been executed properly, as outlined in their computer-system security management plan.

**CI operators are required to have security audits completed every 24 months. submit a report.**

### Cymulate capabilities:

**Assessment reports:** Cymulate assessment dashboards and reports can be used as evidence during computer-system security audits. This assessment data demonstrates how well CI operators are preventing and detecting against the latest emerging cyber threats. The Cymulate platform allows CI operators to continually optimize security controls, fix exploitable vulnerabilities and prove their threat resilience without having to wait for their next assessment or audit to assess their security posture.

# 08

## Participate in Security Drills (Obligation 26)

Obligation 26, categorized as a threat and incident threat and incident preventive measure, requires CI operators to participate in security drills in order to test their state of readiness to respond to security incidents.

**CI operators are required to participate in security drills.**

### Cymulate capabilities:

**Tabletop exercises and simulations:** The Cymulate platform supports cybersecurity tabletops and exercises. Organizations can use the platform to run attack tests and evaluate their processes and capabilities to respond to a security incident, which includes implementing mitigations to improve prevention and detection. The attack test can be run post-mitigation to ensure security controls are mitigating the threats.

09

## Summary

Cymulate empowers organizations to go beyond compliance checklists by continuously validating security controls, identifying exploitable risks and prioritizing mitigation efforts based on actual threats and business impacts. By integrating exposure management into daily operations, CI operators accelerate compliance with Protection of Critical Infrastructure Bill requirements and build lasting cyber threat resilience to minimize disruption to essential services.

Take the next step toward achieving compliance and continuous threat resilience by learning more about the Cymulate Exposure Management Platform.



### About Cymulate

Cymulate is the leader in exposure management that proves the threat and improves resilience. More than 1,000 customers worldwide rely on the Cymulate platform to prove, prioritize and optimize their threat resilience as they make threat validation a continuous process in their exposure management programs. Cymulate integrates with assessment tools and continuously tests defenses against the full kill chain of attack techniques providing cybersecurity teams with the automation and insights to prove and optimize threat resilience; accelerate detection engineering; drive continuous threat exposure management; and measure and baseline security posture. Prove the threat. Improve resilience. For more information, visit [www.cymulate.com](https://www.cymulate.com).

[Get a Demo](#)